UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,060	12/22/2005	Madoka Masugi	450100-04617	4329

7590 09/23/2008

William S Frommer
Frommer Lawrence & Haug
745 Fifth Avenue
New York, NY 10151

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,060	MASUGI ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/13/2007, 12/06/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action in response to application December 22, 2005. Claims (1-75) are pending.

Priority

2. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) - (d) is acknowledged.

The application is filed on December 22, 2005 but is a 371 case of PCT/JP03/06585 application filed 05/27/2003 and has a foreign priority application Japan 2002-167148, Japan 2002-167260, and Japan 2002-167358 filed on 06/07/2002.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 23, 49, and 75 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim limitations are directed to a program stored in memory. A program as recited in claims 23, 49, and 75 respectfully are non-statutory subject matter. Examiner suggests amending the claims to recite, “a program stored on a computer readable storage medium”.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 5-10, 12-15, 17-20, and 22-75 are rejected under 35 U.S.C. 102(e) as being anticipated by Willey et al. (WO 02/063847 A2 and Willey hereinafter).

5. As to claims 1, Willey teaches a **privilege management system for managing service reception privileges of user devices;**

wherein a user device which is a service reception entity holds a group attribute certificate which has (i.e., .. teaches each device a group certificate [abstract, lines 1-6] , **as stored information, group identification information corresponding to a group which is a set of certain devices or certain users** (i.e., … teaches each device has the name the group [abstract, lines 1-6]), **and also has affixed an electronic signature of an issuer** (i.e., ... teaches a certificate signed by CA [abstract, lines 1-6]);

and wherein a service provider (i.e., CA) **which is a service providing entity has a configuration for executing verification, by means of signature verification** (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate presented from said user device regarding whether or not**

there has been tampering (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening** (i.e., discovery) **regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executing determination regarding whether or not service can be provided, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

6. As to claim 2, Willey teaches a **privilege management system where said group attributes certificate is a certificate issued to a user device corresponding to a device or a user** (i.e., …teaches a group certificate issued to a device [pg. 6, lines 30-36]), **under the conditions that mutual authentication is established between a group attributes certificate issuing entity and the user device** (i.e., ... teaches a authentication between CA and device [pg. 10, lines 10-20]), **and that the device or user to which the certificate is to be issued is following an issuance policy permitted by said service provider** (i.e., … teaches a short lived certificate [pg. 10, lines 5-6]).

7. As to claim 3, Willey teaches a **privilege management system where the issuing processing for a new group attributes certificate is of a configuration carried out under the condition that verification is established at the group**

attributes certificate issuing entity regarding an already-issued group attributes certificate which the user device already holds [pg. 3, lines 24-27].

8. As to claim 5, Willey teaches a **privilege management system where said service provider is of a configuration wherein screening** (i.e. discover) **regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

9. As to claim 6, Willey teaches a **privilege management system where said service provider is of a configuration wherein screening** [pg. 4, lines 19-20], **regarding whether or not the object of service permission is executed for first group identification information obtained from a first group attribute certificate based on group definitions from said user device wherein devices are group members** [pg. 4, lines 19-20], **and screening regarding whether or not the object of service permission is executed for second group identification information**

obtained from a second group attribute certificate based on group definitions from said user device wherein devices are group users [pg. 4, lines 19-20], **and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission** [pg. 4, lines 19-20].

10. As to claim 7, Willey teaches a **privilege management system where said user device is of a configuration including an end entity as a device for executing communication with said service provider** (i.e., CA) [50, fig. 1], **and a user identification device as an individual identification device** [110, fig. 1]; **where said group attribute certificate is issued individually to each of said end entity and user identification device** (i.e., …teaches a group certificate issued to a device [pg. 6, lines 30-36]), **with issuing processing being carried out under the condition that mutual authentication has been established between the group attribute certificate issuing entity and said end entity or said user identification device** (i.e., ... teaches a authentication between CA and device [pg. 10, lines 10-20]).

11. As to claim 8, Willey teaches a **privilege management system of a configuration where said group attribute certificate is an attribute certificate issued by an attribute authority** [pg. 4, lines 19-20], **and a group identifier is stored in an attribute information filed within the attribute certificate** (i.e., … teaches each device has the name the group [abstract, lines 1-6]).

12. As to claim 9, Willey teaches a **privilege management system where said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate (i**.e., ... teaches a public key [pg. 9, lines 25-35]);

and where said service provider is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate (i.e., … teaches verification using public and private key [pg. 9, lines 25-35].

13. As to claim 10, Willey teaches a **information processing device for executing data processing as service providing processing, comprising: a data reception unit for receiving a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer** [fig. 1; abstract lines 1-6];

and a group attribute certificate verification processing unit (i.e., CA) **for executing verification, by means of signature verification** (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening regarding whether or not this is a service-permitted group based on group identification information**

stored in said group attribute certificate (i.e., … teaches a service discovery process for devices [pg, 13, lines 25-30])**, and executing determination regarding whether or not service can be provided, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

14. As to claim 12, Willey teaches a **information processing device where said group attribute certificate verification processing unit is of a configuration wherein screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device, and determining processing regarding whether or not service can be provided is executed** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]).

15. As to claim 13, Willey teaches a **privilege management method for managing service reception privileges of user devices, comprising: as an execution step at a user device which is a service reception entity, a step for transmitting to a service provider which is a service providing entity a group attribute certificate which has** (i.e., … teaches transmitting to a CA [pg. 10, lines 10-15]), **as stored information, group identification information corresponding to a group**

which is a set of certain devices or certain users (i.e., … teaches each device has the name the group [abstract, lines 1-6]), **and also has affixed an electronic signature of an issuer** [abstract, lines 1-6];

and, as an execution step at said service provider, a step for performing verification, by means of signature verification (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate presented from said user device regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executing determination regarding whether or not service can be provided, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

16. As to claim 14, Willey teaches a **privilege management method further comprising a group attribute certificate issuing processing step for issuing said group attributes certificate to a user device corresponding to a device or a user** [pg. 3, lines 24-27];

where said group attribute certificate issuing processing step is a processing step for issuing the group attribute certificate to a user device corresponding to a device or a user under the conditions that mutual

authentication is established between a group attributes certificate issuing entity and the user device [pg. 7, lines 10-20], **and that the device or user to which the certificate is to be issued is following an issuance policy permitted by said service provider** [pg. 7, lines 15-20].

17. As to claim 15, Willey teaches a **privilege management method where said group attribute certificate issuing processing step includes a verification processing step regarding an already-issued group attributes certificate which the user device already holds, wherein issuing of a group attributes certificate is carried out under the condition that said verification is established** [pg. 9, lines 25-35].

18. As to claim 17, Willey teaches a **privilege management method where service provider is of a configuration wherein screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission** (i.e., … teaches making determination for purpose of

verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

19. As to claim 18, Willey teaches a **privilege management method where at said service provider, screening regarding whether or not the object of service permission is executed for first group identification information obtained from a first group attribute certificate based on group definitions from said user device wherein devices are group members** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and screening regarding whether or not the object of service permission is executed for second group identification information obtained from a second group attribute certificate based on group definitions from said user device where devices are group users** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30])**, and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission** (i.e., … teaches multiple group configuration for which permission verification as prescribed using a certificate privilege base discovery process [fig. 3]).

20. As to claim 19, Willey teaches a **privilege management method where said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate** [pg. 7, lines 25-35];

and where said service provider is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate [pg. 7, lines 25-35].

21. As to claim 20, Willey teaches a **information processing method for an information processing device for executing data processing as service providing processing, said method comprising:**

a certificate reception step for receiving from a service providing device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer, as an attribute certificate to be applied to service usage privilege confirmation processing [abstract, lines 1-6[

and a group attribute certificate verification processing step for executing verification, by means of signature verification of the group attribute certificate (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate**(i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executing determination regarding whether or**

not service can be provided, based on said screening (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

22. As to claim 22, Willey teaches a **information processing method where said group attribute certificate verification processing step includes a step for executing screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device** (i.e., … teaches group certificate for authentication [pg. 6, lines 34-35] .... teaches a group certificates identifies devices as part of a privilege group (i.e., **screening**)), **and executing determining processing regarding whether or not service can be provided under the condition that all group identification sets are the object of service permission** (i.e., … teaches depending on devices application (i.e., **services**) such that determination of processing (i.e., **screening**) accessibility may be decline [pg. 7, lines 5-10]).

23. As to claim 23, Willey teaches a **computer program for effecting execution of privilege management processing for managing service reception privileges of user devices, said program comprising:**

a certificate reception step for receiving from a service providing device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer, as an attribute certificate to be applied to service usage privilege confirmation processing [abstract, lines 1-6];

and a group attribute certificate verification processing step for executing verification, by means of signature verification of the group attribute certificate (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening** (i.e., discovery) **regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executing determination regarding whether or not service can be provided, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

24. As to claim 24, Willey teaches a **access privilege management system for executing access restrictions between communication devices having communication functions;**

where an access requesting device stores, in storage means, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer [abstract, lines 1-6];

and where an access requested device, which is the object of an access request from said access requesting device, executes verification, by means of signature verification (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate presented from said access requesting device regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executes determination regarding whether or not access can be permitted, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

25. As to claim 25, Willey teaches a **access privilege management system where said access requested device has a configuration for performing screening regarding whether or not said access requesting device is an end entity**

belonging to an access-permitted group (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **based on a group attribute certificate issued to the end entity which is an access executing device making up said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

26. As to claim 26, Willey teaches a **access privilege management system according to claim 24, wherein said access requested device has a configuration for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

27. As to claim 27, Willey teaches a **access privilege management system of a configuration wherein said access requesting device and said access requested**

device have security chips with anti-tampering configurations, with mutual authentication being executed between the mutual security chips (i.e., … teaches mutual authentication between devices [pg. 6, lines 34-35], **and where, under the condition that mutual authentication has been established, said access requested device executes signature verification of the group attribute certificate presented from said access requesting device** [pg. 9, lines 25-32], **and screening regarding whether or not the device belongs to an access-permitted group** [pg. 13, lines 30-35].

28. As to claim 28, Willey teaches a **access privilege management system of a configuration wherein said access requested device receives from a device an issuing request for a group attribute certificate certifying that the device is an access-permitted group member** [pg. 10, lines 10-15];

and where, under the conditions that mutual authentication between devices has been established and that the group attribute certificate issue requesting device is following an issuance policy permitted by said access requested device [pg. 18, lines 15-25], **issues a group attribute certificate to a device corresponding to a device or a user** [pg. 16, lines 5-7], **certifying that the device is an access-permitted group member** [pg. 13, lines 30-35].

29. As to claim 29, Willey teaches a **access privilege management system of a configuration wherein said access requested device receives from a device an**

issuing request for a group attribute certificate certifying that the device is an access-permitted group member (i.e., … teaches the root key of the members' CA defines the membership of a group; all devices having certificates signed by the same CA's private key comprise a group [pg. 7, lines 20-25]);

and where, under the conditions that mutual authentication between devices has been established and that verification and screening is established for an already-issued group attribute certificate already held by the group attribute certificate issue requesting device, issues a group attribute certificate to a device corresponding to a device or a user, certifying that the device is an access-permitted group member [pg. 7,lines 10-25].

30. As to claim 30, Willey teaches a **access privilege management system where said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate** [pg. 7, lines 25-35];

and where said access requesting device is of a configuration where verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate [pg. 7, lines 25-35].

31. As to claim 31, Willey teaches a **communication processing device for executing access restriction processing, comprising:**

a reception unit for receiving, from an access requesting device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer [abstract, lines 1-6];

and an access privilege determination processing unit for executing group attribute certificate verification processing functions, for executing verification, by means of signature verification (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification**
32. **information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **and executing determination regarding whether or not access can be permitted, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

33. As to claim 32, Willey teaches a **communication processing device where said access privilege determination processing unit has a configuration for performing screening regarding whether or not said access requesting device is**

an end entity belonging to an access-permitted group (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]), **based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

34. As to claim 33, Willey teaches a **communication processing device where said access privilege determination processing unit has a configuration for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group** (i.e., … teaches the root key of the members' CA defines the membership of a group; all devices having certificates signed by the same CA's private key comprise a group [pg, 9, lines 25-35]), **based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device** [pg, 9, lines 25-35], **and executing determination regarding whether or not access can be permitted, based on said screening** [pg, 9, lines 25-35].

35. As to claim 34, Willey teaches a **communication processing device comprising an encipherment processing unit for executing mutual authentication with said access requesting device;**

where said access privilege determination processing unit has a configuration for, under the condition that mutual authentication has been established (i.e., ... teaches a authentication between CA and device [pg. 10, lines 10-20]) , **executing signature verification of the group attribute certificate presented from said access requesting device** (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **and screening regarding whether or not the device belongs to an access-permitted group** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]).

36. As to claim 35, Willey teaches a **communication processing device further comprising an attribute certificate generating unit for generating a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer** [abstract, lines 1-6].

37. As to claim 36, Willey teaches a **communication processing device where said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate** [pg. 9, lines 25-35];

and where said access privilege determination processing unit is of a configuration wherein verification of the public key certificate obtained by said

link information is also executed at the time of performing verification of said group attribute certificate [pg. 9, lines 25-35]

38. As to claim 37, Willey teaches a **access privilege management method for executing access restrictions between communication devices having communication functions, said method comprising:**

a step for an access requesting device to transmit to an access requested device, which is the object of an access request, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer [abstract, lines 1-6];

a step for said access requested device to receive the group attribute certificate presented by said access requesting device;

a screening step for executing verification, by means of signature verification (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate presented from said access requesting device regarding whether or not there has been tampering** (i.e., …teaches certificate validity determination [pg. 18, lines 5-25]), **and performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30]);

and a step for executing determination regarding whether or not access can be permitted, based on the screening results in said screening step (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [pg. 9, lines 30-35]).

39. As to claim 38, Willey teaches a **access privilege management where said access requested device performs screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group** (i.e., ... teaches a first device authenticating a second device [pg. 3, lines 30-33]), **based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device** (i.e., … teaches each device maintains a CRL for purpose of authentication [pg. 4, lines 23-27], **and executing determination regarding whether or not access can be permitted, based on said screening** [pg. 16, lines 20-25].

40. As to claim 39, Willey teaches a **access privilege management method where said access requested device performs screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group** [pg. 7, lines 20-25], **based on a group attribute certificate issued to a user identification device which is an individual identification device at said access requesting device** [pg. 7, lines 20-25], **and executing determination regarding whether or not access can be permitted, based on said screening** (i.e.,

… teaches the root key of the members' CA defines the membership of a group; all devices having certificates signed by the same CA's private key comprise a group [pg. 7, lines 20-25]).

41. As to claim 40, Willey teaches a **access privilege management method further comprising a mutual authentication execution step between security chips with anti-tampering configurations of said access requesting device and said access requested device** (i.e., … teaches … further teaches devices all have embedded in memory the public key associated with the private key in the tamper-proof hardware of TS [pg. 17, lines 30-34]);

where, under the condition that mutual authentication has been established, said access requested device executes signature verification of the group attribute certificate presented from said access requesting device [pg. 18, lines 15-21], and screening regarding whether or not the device belongs to an access-permitted group (i.e., … teaches exchanging certificates as part of authentication [pg. 18, lines 20-25] ... teaches each device maintains a list of participating device [abstract]).

42. As to claim 41, Willey teaches a **access privilege management method further comprising a step for said access requested device to receive from a device an issuing request for a group attribute certificate certifying that the device is an**

access-permitted group member (i.e., … teaches exchanging certificates as part of authentication [pg. 18, lines 20-25]);

and a step where, under the conditions that mutual authentication between devices has been established and that the group attribute certificate issue requesting device is following an issuance policy permitted by said access requested device [pg. 7, lines 15-20], **a group attribute certificate is issued to a device corresponding to a device or a user** [pg. 7, lines 10-16].

43. As to claim 42, Willey teaches a **access privilege management method further comprising, as an execution step at said access requested device in response to an issuing request from a device for a group attribute certificate certifying that the device is an access-permitted group member** [pg. 7, lines 10-16], a step for executing processing for issuing a group attribute certificate to a device corresponding to a device or a user [pg. 7, lines 10-16], **certifying that the device is an access-permitted group member, under the conditions that mutual authentication between devices has been established and that verification and screening is established for an already-issued group attribute certificate already held by the group attribute certificate issue requesting device** [pg. 7, lines 15-20].

44. As to claim 43, Willey teaches a **access privilege management method where said group attribute certificate is of a configuration storing link information**

regarding a public key certificate corresponding to said group attribute certificate [pg. 9, lines 25-35];

and where said access requesting device is of a configuration where verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate [pg. 9, lines 25-35].

45. As to claim 44, Willey teaches a **communication managing method for a communication processing device for executing access restriction processing, said method comprising: a reception step for receiving, from an access requesting device, a group attribute certificate which has, as stored information** [pg. 20, lines 5-15], **group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer** [abstract, lines 1-6];

and an access privilege determination processing step for executing verification, by means of signature verification (i.e., … teaches a CA verification of the signature [pg, 9, lines 25-35]), **of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering, performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate** [pg. 22, lines 5-10];

and an access permissible/impermissible determination step for executing determination regarding whether or not access can be permitted, based on the access privilege determination processing results [pg. 6, lines 34-35].

46. As to claim 45, Willey teaches **a communication managing method where said access privilege determination processing step includes a step performing screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group, based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device** [pg. 7, lines 20-25].

47. As to claim 46, Willey teaches a **communication managing method where said access privilege determination processing step includes a step for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group, based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device** [pg. 7, lines 20-25].

48. As to claim 47, Willey teaches a **communication managing method further comprising an authentication processing step for executing mutual authentication with said access requesting device** [pg. 6, lines 34-35];

where, in said access privilege determination processing step, signature verification of the group attribute certificate presented from said access requesting device, and screening regarding whether or not the device belongs to an access-permitted group, are executed, under the condition that mutual authentication has been established [pg. 18, lines 15-21].

49. As to claim 48, Willey teaches a **communication managing method where said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate** [pg. 9, lines 25-35];

and where, in said access privilege determination processing step, verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate [pg. 9, lines 25-35].

50. As to claim 49, Willey teaches a **computer program for effecting execution of a communication managing method for a communication processing device for executing access restriction processing, said program comprising:**

a reception step for receiving, from an access requesting device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication

devices or certain users, and also has affixed an electronic signature of an issuer [abstract, line 1-6];

and an access privilege determination processing step for executing verification, by means of signature verification, of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering [pg. 18, lines 15-21], **performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate** [pg. 6, lines 34-35] ;

and an access permissible/impermissible determination step for executing determination regarding whether or not access can be permitted, based on the access privilege determination processing results [pg. 6, lines 34-35].

51. As to claim 50, Willey teaches a **data processing system for executing data processing accompanied by data communication processing, between a plurality of devices capable of mutual communication** [fig. 1], **where, of said plurality of devices, a data processing requesting device, which requests data processing to the other device with which communication is being made, holds a group attribute certificate which has, as stored information** [pg, 7, lines 19-20], **group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer** [abstract, lines 1-6], **and transmits said group attribute certificate to a data**

processing requested device at the time of data processing requesting processing [pg. 7, lines 30-32];

and wherein said data processing requested device executes verification processing of the received group attribute certificate [pg. 7, lines 30-32], **determines whether or not said data processing requesting device has data processing requesting privileges based on said verification, and executes data processing based on determination of privileges** [pg. 6, lines 34-35].

52. As to claim 51, Willey teaches a **data processing system where the group attribute certificate stored in said data processing requesting device has as the issuer thereof the data processing requested device, and has affixed the electronic signature of the data processing requested device** [abstract, lines 1-6];

and where said data processing requested device is of a configuration for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate [pg. 9, lines 25-35].

53. As to claim 52, Willey teaches a **data processing system where all of said mutually communicable plurality of devices are devices which mutually request data processing of the other device with which communication is being made, with each of the devices having a configuration storing the group attribute certificate issued by the communication party device and transmitting the group**

attribute certificate stored in itself at the time of data processing requesting of the other device with which communication is being made, and under the condition of verification being established at the receiving device, processing corresponding to the data processing request is mutually executed [pg. 18, lines 10-25].

54. As to claim 53, Willey teaches **a data processing system where all of said mutually communicable plurality of devices have security chips with anti-tampering configurations** [pg. 17, lines 30-34], **with mutual authentication being executed between the mutual security chips at the time of data processing requesting of the other device with which communication is being made** [pg. 18, lines 20-25], **and where, under the condition that mutual authentication has been established, said transmission of group attribute certificates between the devices, and verification of the transmitted group attribute certificates, is executed** [pg. 18, lines 20-25].

55. As to claim 54, Willey teaches a **data processing system where the group attribute certificate stored in the data processing requesting device has as the issuer thereof the data processing requested device** (i.e., … teaches Certificate Authority (CA) 50 is responsible for issuing short-lived certificates to the devices and for sending the short-lived certificates to the devices upon request [pg. 7, lines 10-20]);

and where issuing processing is performed under the condition that mutual authentication has been established between the data processing requesting device and the data processing requested device (i.e., … teaches the validity of a certificate depends upon the current time, devices have accurate time sources that are always available for validating certificates. … teaches, devices are distinguished as members of an ad-hoc group by giving the group a name, make all of the devices aware of the group name, and include the name in the certificates signed by the CA. … further teaches when the devices check a certificate for the purpose of authenticating a fellow ad-hoc group member, they will verify that the certificate contains the group name [pg. 7, lines 10-20]).

56. As to claim 55, Willey teaches a **data processing system where said mutually communicable plurality of devices, at least one or more devices comprise, as a device configuration, an end entity for executing communication processing with other device and data processing, and a user identification device having individual identification functions capable of exchanging data with said end entity** [pg. 18, lines 20-25];

and where, in the event that said group attribute certificate is issued to members making up a certain user group [pg. 7, lines 10-15], **issuing processing is carried out under the condition that mutual authentication is established between said user identification device and a group attribute certificate issuing processing**

executing device (i.e., … teaches a members certificates are signed by CA [pg. 7, lines 10-15]).

57. As to claim 56, Willey teaches a **data processing system where said mutually communicable plurality of devices** [pg. 6, lines 34-35], one is a maintenance executing device for executing maintenance processing for devices (i.e., ... teaches CA provides tracking (i.e., **maintenance**) capability [pg. 9, lines 25-30]);

and where the other devices are service receiving device which receive the maintenance service from said maintenance executing device (i.e., … teaches a devices receiving a short-lived certificates from CA [pg. 9, lines 10-15];

and where said service receiving device stores a service attribute certificate which is a group attribute certificate issued by said maintenance executing device [pg. 3, lines 30-33];

and where said maintenance executing device stores a control attribute certificate which is a group attribute certificate issued by said service receiving device [pg. 9, lines 10-15]; **and where said service attribute certificate is applied for verification at said maintenance executing device that said service receiving device belongs to a group of devices or users having maintenance service receiving privileges** [pg. 6, lines 34-35];

and where said control attribute certificate is applied for verification at said service receiving device that said maintenance executing device belongs to a

group of devices or users having maintenance service executing privileges [pg. 7, lines 19-25].

58. As to claim 57, Willey teaches a **data processing system where a maintenance program executed at said service receiving device is transmitted to or stored in said service receiving device as an enciphered maintenance program** [pg. 3, lines 30-33];

and where said service receiving device is of a configuration for deciphering said enciphered maintenance program within a security chip having an anti-tampering configuration (i.e., … teaches devices all have embedded in memory the public key associated with the private key in the tamper-proof hardware of TS [pg. 17, lines 30-34])**, and then executing on said service receiving device**.

59. As to claim 58, Willey teaches a **data processing system where maintenance processing executed at said service receiving device is executed based on commands transmitted from said maintenance executing device to said service receiving device** [pg. 18, lines 10-19];

and where said service receiving device transmits a response to said maintenance executing device for the execution results of said commands, and said maintenance executing device executes transmission of new commands to said service receiving device based on the transmitted response [pg. 18, lines 10-19].

60. As to claim 59, Willey teaches a **data processing device for executing data processing based on data processing requests from a data processing requesting device, said data processing device comprising:**

a data reception unit for receiving from said data processing requesting device a group attribute certificate which has, as stored information [pg. 7, lines 10-15], **group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer** [abstract, lines 1-6];

a privilege determining processing unit for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification [pg. 6, lines 34-35];

and a data processing unit for executing data processing based on determination of privileges [pg. 6, lines 34-35].

61. As to claim 60, Willey teaches a **data processing device where said privilege determining processing unit is of a configuration for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate** [pg. 9, lines 25-35].

62. As to claim 61, Willey teaches a **data processing device where said data processing device has a security chip with an anti-tampering configuration and comprising an enciphering processing unit;**

and where said enciphering processing unit has a configuration wherein mutual authentication is executed with the data processing requesting device in response to a data processing request from the data processing requesting device [pg. 7, lines 10-20];

and where said privilege determining processing unit is of a configuration for executing verification of the group attribute certificate, under the condition that mutual authentication has been established [pg. 7, lines 10-20].

63. As to claim 62, Willey teaches a **data processing device where said data processing device is of a configuration comprising an attribute certificate generating processing unit having functions for generating a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature** [abstract, lines 1-6].

64. As to claim 63, Willey teaches a **data processing method for executing data processing accompanied by data communication processing, between a plurality of devices capable of mutual communication** [fig. 1], **where, of said plurality of devices, a data processing requesting device, which requests data processing to**

the other device with which communication is being made, executes a step for transmitting, to the other device with which communication is being made at the time of data processing requesting processing, a group attribute certificate which has, as stored information [pg, 7, lines 19-20], **group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer** [abstract, lines 1-6];

and where said data processing requested device executes: a verification processing step for the received group attribute certificate [pg. 7, lines 30-32];

a step for determining whether or not said data processing requesting device has data processing requesting privileges based on said verification [pg. 6, lines 34-35];

and a step for executing data processing based on determination of privileges [pg. 20, lines 28-31].

65. As to claim 64, Willey teaches a **data processing method where the group attribute certificate stored in said data processing requesting device has as the issuer thereof the data processing requested device, and has affixed the electronic signature of the data processing requested device** [abstract, lines 1-6];

and where, in said verification processing step at said data processing requested device, electronic signature verification processing applying a public key of itself is executed, as verification processing of the received group attribute certificate [pg. 9, lines 25-35].

66. As to claim 65, Willey teaches a **data processing method where all of said mutually communicable plurality of devices are devices which mutually request data processing of the other device with which communication is being made, with each of the devices having a configuration storing the group attribute certificate issued by the communication party device and transmitting the group attribute certificate stored in itself at the time of data processing requesting of the other device with which communication is being made, and under the condition of verification being established at the receiving device, processing corresponding to the data processing request is mutually executed** (i.e., ... teaches mutual authentication [pg. 16, lines 20-25]).

67. As to claim 66, Willey teaches a **data processing method where all of said mutually communicable plurality of devices have security chips with anti-tampering configurations** [pg. 17, lines 29-34], **with mutual authentication being executed between the mutual security chips at the time of data processing requesting of the other device with which communication is being made, and where, under the condition that mutual authentication has been established, said transmission of group attribute certificates between the devices, and verification of the transmitted group attribute certificates, is executed** (i.e., ... teaches mutual authentication [pg. 16, lines 20-25]).

68. As to claim 67, Willey teaches a **data processing method further comprising an issuing processing step for the group attribute certificate stored in the data processing requesting device** [pg. 3, lines 30-33]**;**

said issuing processing step being executed under the condition that mutual authentication has been established between the data processing requesting device and the data processing requested device [pg. 16, lines 20-25].

69. As to claim 68, Willey teaches a **data processing method further comprising an issuing processing step for the group attribute certificate stored in the data processing requesting device** [pg. 3, lines 30-33];

where, in the event that said group attribute certificate is issued to members making up a certain user group, said issuing processing step is executed under the condition that mutual authentication is established with a user identification device having individual identification functions making of the data processing requesting device [pg. 16, lines 20-25].

70. As to claim 69, Willey teaches a **data processing method where, of said mutually communicable plurality of devices, one is a maintenance executing device for executing maintenance processing for devices, and wherein the other devices are service receiving device which receive the maintenance service from said maintenance executing device, said method comprising:**

a step for said service receiving device to transmit to said maintenance executing device a service attribute certificate which is a group attribute certificate issued by said maintenance executing device [par. 26];

a service attribute certificate verification step for said maintenance executing device to execute verification of the received service attribute certificate [par. 26];

a step for said maintenance executing device to transmit to said service receiving device a control attribute certificate which is a group attribute certificate issued by said service receiving device (i.e., … teaches the functions of issuing short-lived certificates to the devices and for sending the short-lived certificates to the devices [par. 26]);

a control attribute certificate verification step for said service receiving device to execute verification of said control attribute certificate (i.e., … teaches CA would act as an OCSP responder and upon request from the OCSP client would indicate whether or not a public key/private key pair is valid [par. 26]);

and a maintenance processing step for executing maintenance processing under the condition that both verification of said service attribute certificate verification and said control attribute certificate verification have been established (i.e., … teaches he OCSP client would issue a precomputed OCSP response only if the CA indicates that the public key/private key pair is valid [par. 26]).

71. As to claim 70, Willey teaches a **data processing method where a maintenance program executed at said service receiving device is transmitted to or stored in said service receiving device as an enciphered maintenance program** [pg. 3, lines 30-33];

and where said service receiving device is of a configuration for deciphering said enciphered maintenance program within a security chip having an anti-tampering configuration, and then executing on said service receiving device (i.e., … teaches a tamper-proof configuration [pg. 17, lines 29-34]).

72. As to claim 71, Willey teaches a **data processing method where maintenance processing executed at said service receiving device is executed based on commands transmitted from said maintenance executing device to said service receiving device** [pg. 16, lines 10-21];

and where said service receiving device transmits a response to said maintenance executing device for the execution results of said commands, and said maintenance executing device executes transmission of new commands to said service receiving device based on the transmitted response [pg. 16, lines 10-21].

73. As to claim 72, Willey teaches a **data processing method for executing data processing based on data processing requests from a data processing requesting device, said method comprising:**

a data reception step for receiving from said data processing requesting device a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer [abstract, lines 1-6];

a privilege determining processing step for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification [pg. 16, lines 20-25];

and a data processing step for executing data processing based on determination of privileges [pg. 20, lines 28-31].

74. As to claim 73, Willey teaches a **data processing method where said privilege determining processing step includes a step for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate** [pg. 9, lines 25-35].

75. As to claim 74, Willey teaches a **data processing method further comprising a step for executing mutual authentication with the data processing requesting device in response to a data processing request from the data processing requesting device;**

and wherein said privilege determining processing step executes verification of the group attribute certificate, under the condition that mutual authentication has been established [pg. 16, lines 20-25].

76. As to claim 75, Willey teaches a **computer program for effecting execution of data processing based on data processing requests from a data processing requesting device, said program comprising:**

a data reception step for receiving from said data processing requesting device a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer [abstract, lines 1-6];

a privilege determining processing step for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification [pg. 16, lines 20-25];

and a data processing step for executing data processing based on determination of privileges [pg. 20, lines 28-31].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

77. Claims 4, 11, 16, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Willey in view of Adams (US Patent No. 6,718,470).

78. As to claim 4, Willey teaches a **privilege management system where said service provider is of a configuration having a group information database wherein said group identifier and permitted service information for members belonging to the group are correlated** [i.e., .. teaches CA is responsible for defining group memberships [pg. 7, lines 20-25]), **and determining processing regarding**

whether or not service can be provided is executed (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30])

However Willey does not expressly teach:

where said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Willey as introduced by Adams. Adams discloses:

where said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device (for purposes of privilege management Adams provides the ability to search a local store containing privilege information [col. 7, lines 25-35]),

Therefore, given the teachings of Adams, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Willey by employing the well known features of searching a certificate database disclosed above by Adams, for which privilege management will be enhanced [col. 7, lines 25-35].

79. As to claim 11, Willey teaches a **information processing device of a configuration further comprising a group information database** (i.e., CRL) **in said group identifier and permitted service information for members belonging to the group are correlated** [pg. 4, lines 20-30]; **and executes determining processing regarding whether or not service can be provided** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30])

However Willey does not expressly teach:

where said group attribute certificate verification processing unit searches said group information database based on the group identification information stored in said group attributes certificate presented by said user device,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Willey as introduced by Adam. Adam discloses:

where said group attribute certificate verification processing unit searches said group information database based on the group identification information stored in said group attributes certificate presented by said user device (for purposes of privilege management Adam provides the ability to search a database containing client information [col. 7, lines 25-35]),

Therefore, given the teachings of Adam , a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Willey by employing the well known features of searching a certificate database disclosed above by Adam , for which privilege management will be enhanced [col. 7, lines 25-35].

80. As to claim 16, Willey teaches **a privilege management method where said service provider is of a configuration having a group information database wherein said group identifier and permitted service information for members belonging to the group are correlated** (i.e., … teaches the root key of the members' CA defines the membership of a group; all devices having certificates signed by the same CA's private key comprise a group [par. 25], **and determining processing regarding whether or not service can be provided is executed** (i.e., … teaches making determination for purpose of verification such that determination allows continual participation in network [col. 7, lines 25-35]).

However Willey does not expressly teach:

where said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Willey as introduced by Adam. Adam discloses:

where said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device (for purposes of privilege management Adam provides the ability to search a database containing client information [col. 7, lines 25-35]),

Therefore, given the teachings of Adam , a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Willey by employing the well known features of searching a certificate database disclosed above by Adam, for which privilege management will be enhanced [col. 7, lines 25-35].

81. As to claim 21, Willey teaches a **information processing method said information processing device further comprising a group information database where said group identifier and permitted service information for members belonging to the group are correlated** (i.e., … teaches a CRL [pg. 4, liens 20-30]); **and executing determining processing regarding whether or not service can be provided** (i.e., .. teaches a service discovery process for devices [pg, 13, lines 25-30])

However Willey does not expressly teach:

where said group attribute certificate verification processing step includes a step for searching said group information database based on the group identification information stored in said group attributes certificate presented by said user device,

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Willey as introduced by Adam. Adam discloses:

where said group attribute certificate verification processing step includes a step for searching said group information database based on the group identification information stored in said group attributes certificate presented by said user device (for purposes of privilege management Adam provides the ability to search a database containing client information [col. 7, lines 25-35]),

Therefore, given the teachings of Adam , a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Willey by employing the well known features of searching a certificate database disclosed above by Adam , for which privilege management will be enhanced [col. 7, lines 25-35].

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131